CLAIMS

What is claimed is:

1   1.   A method, comprising the computer-implemented steps of:
2   determining a user identifier associated with a network device that has caused a
3   security event in a network;
4   causing the network device to receive a network address that is selected from a subset
5   of addresses within a specified pool associated with suspected malicious
6   network users; and
7   configuring one or more security restrictions with respect to the selected network
8   address.

1   2.   A method as recited in Claim 1, further comprising the steps of:
2   receiving information identifying the security event in the network;
3   correlating the security event information with network user information to result in
4   determining the user identifier associated with the network device.

1   3.   A method as recited in Claim 1, wherein the network device uses dynamic host
2   control protocol (DHCP) to obtain the network address, and wherein the step of causing the
3   network device to receive a network address comprises resetting a port that is coupled to the
4   network device to prompt a user to command the network device to request a new network
5   address using DHCP.

1   4.   A method as recited in Claim 1, wherein the network device uses dynamic host
2   control protocol (DHCP) to obtain the network address, and wherein the step of causing the
3   network device to receive a network address comprises issuing a DHCP FORCE_RENEW
4   message to the network device.

-20-

1 5.   A method as recited in Claim 1, wherein the network device uses dynamic host
2 control protocol (DHCP) to obtain the network address, and wherein the step of causing the
3 network device to receive a network address comprises prompting the network device to
4 request a new network address using DHCP.

1 6.   A method as recited in Claim 1, wherein the network device uses dynamic host
2 control protocol (DHCP) to obtain the network address, and wherein the step of causing the
3 network device to receive a network address comprises waiting for expiration of a lease for a
4 current network address of the network device.

1 7.   A method as recited in Claim 1, wherein the step of causing the network device to
2 receive a network address comprises the step of providing the network device with an IP
3 address that is selected from a plurality of IP addresses within a special IP subnet.

1 8.   A method as recited in Claim 7, further comprising the step of publishing information
2 describing characteristics of the special IP subnet to network service providers.

1 9.   A method as recited in Claim 1, wherein the step of configuring security restrictions
2 comprises the steps of modifying an internet protocol (IP) access control list (ACL)
3 associated with a port that is coupled to the network device to permit entry of IP traffic from
4 only the selected network address.

1 10.   A method as recited in Claim 1, wherein the step of configuring security restrictions
2 comprises the steps of modifying a media access control (MAC) ACL associated with a port
3 that is coupled to the network device to permit entry of traffic only for a MAC address that is
4 bound to the selected network address.

50325-0865 (Seq. No. 8349)

1 11.   A method as recited in Claim 1, further comprising the steps of determining whether
2 a malicious act caused the security event, and if so, providing information about the security
3 event or malicious act to a security decision controller.

1 12.   A method as recited in Claim 1, further comprising the steps of determining whether
2 a malicious act caused the security event, and if not, removing the user from the elevated risk
3 group.

1 13.   A method as recited in Claim 1, further comprising the steps of determining whether
2 a malicious act caused the security event, wherein a legal user action in the network is not
3 determined to be a malicious act if the user is associated with a trusted customer of a network
4 service provider.

1 14.   A method, comprising the computer-implemented steps of:
2   receiving information identifying a security event in a network;
3   correlating the security event information with network user information to result in
4   determining a network user associated with the network device.
5   placing the user in an elevated risk security group;
6   configuring one or more security restrictions with respect to the selected network
7   address;
8   determining whether a malicious act caused the security event;
9   if a malicious act caused the security event, then providing information about the
10   security event or malicious act to a security decision controller;
11   if a malicious act did not cause the security event, then removing the user from the
12   elevated risk group.

50325-0865 (Seq. No. 8349)

1 15.   A method as recited in Claim 14, wherein placing the user identifier in an elevated
2 risk security group further comprises the step of forcing the user to acquire a new network
3 address from a specified group of network addresses that is reserved for users associated with
4 elevated user risk;

1 16.   A method as recited in Claim 15, wherein forcing the user to acquire a new network
2 address comprises the steps of:
3   re-configuring a dynamic host control protocol (DHCP) server to require said server
4   to issue any new network address to the network device only from a specified
5   group of network addresses that is reserved for users associated with elevated
6   user risk;
7   performing any one of the steps of:
8   (a) resetting a port that is coupled to the network device to trigger the network
9   device to request a new network address using DHCP;
10   (b) issuing a DHCP FORCE_RENEW message to the network device;
11   (c) prompting the network device to request a new network address using DHCP;
12   (d) waiting for expiration of a lease for a current network address of the network
13   device.

1 17.   A method as recited in Claim 14, wherein the step of configuring one or more
2 security restrictions comprises the steps of:
3   modifying an internet protocol (IP) access control list (ACL) associated with a port
4   that is coupled to the network device to permit entry of IP traffic from only
5   the selected network address;
6   modifying a media access control (MAC) ACL associated with the port to permit
7   entry of traffic only for a MAC address that is bound to the selected network
8   address.

1   18.   A computer-readable medium carrying one or more sequences of instructions, which
2   instructions, when executed by one or more processors, cause the one or more processors to
3   carry out the steps of:
4   determining a user identifier associated with a network device that has caused a
5   security event in a network;
6   causing the network device to receive a network address that is selected from a subset
7   of addresses within a specified pool associated with suspected malicious
8   network users; and
9   configuring one or more security restrictions with respect to the selected network
10   address.

1   19.   An apparatus, comprising:
2   means for determining a user identifier associated with a network device that has
3   caused a security event in a network;
4   means for causing the network device to receive a network address that is selected
5   from a subset of addresses within a specified pool associated with suspected
6   malicious network users; and
7   means for configuring one or more security restrictions with respect to the selected
8   network address.

1   20.   An apparatus, comprising:
2   a network interface that is coupled to the data network for receiving one or more packet
3   flows therefrom;
4   a processor;
5   one or more stored sequences of instructions which, when executed by the processor, cause
6   the processor to carry out the steps of:
7   determining a user identifier associated with a network device that has caused a
8   security event in a network;

50325-0865 (Seq. No. 8349)

9 causing the network device to receive a network address that is selected from a subset

10   of addresses within a specified pool associated with suspected malicious

11   network users; and

12 configuring one or more security restrictions with respect to the selected network

13   address.